

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Stubblebine April 20, 2001
Serial No.: Cont. of 09/689859 Group Art Unit: Unassigned
Filed: Herewith Examiner: Unassigned
For: SPECIFYING SECURITY PROTOCOLS AND POLICY CONSTRAINTS IN
DISTRIBUTED SYSTEMS

PRELIMINARY AMENDMENT

Honorable Assistant Commissioner
of Patents and Trademarks
Washington, D.C. 20231
Sir:

Please amend the above-identified continuation application as follows. No new matter is added.

I. IN THE CLAIMS

Please CANCEL claim 1.

Please ADD the following NEW claims:

52. (NEW) A method for system security in distributed systems, comprising the steps of:

- a) deriving freshness constraints from initial policy assumptions and an authentic statement;
- b) imposing freshness constraints by employing recent-secure authenticating principals to effect revocation; and
- c) verifying that a relation $|t_{now} - t_{time\ stamp}| \leq \delta$ is satisfied for verification of a secure channel, where $t_{time\ stamp}$ being a time of a time stamp pertaining to a validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification.

53. (NEW) A system for enforcing revocation in distributed systems, comprising:

- a) means for asserting a time stamped validity assertion pertaining to the validity of an initial assertion;
- b) means for asserting freshness constraints indicating a length of time and the initial assertions that the freshness constraints relate to; and
- c) means for verifying that a relation $|t_{now} - t_{time\ stamp}| \leq \delta$ is satisfied for each particular assertion necessary for verification of a secure channel, where $t_{time\ stamp}$ is a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification.

54. (NEW) A system for protecting an authority of a distinguished principal and enforcing revocation when the authority is compromised, comprising:

- a) means for issuing an authoritative assertion by a distinguished principal;
- b) means for asserting freshness constraints on the assertion;
- c) means for asserting a time stamped validity assertion to the assertion indicating the validity of the assertion at the time of the time stamp; and
- d) means for verifying that a relation $|t_{now} - t_{time\ stamp}| \leq \delta$ is satisfied for each particular assertion necessary for verification of a secure channel, where $t_{time\ stamp}$ being the time of a time stamp pertaining to the validity assertion of the particular assertion, δ being the minimum necessary freshness constraint pertaining to the particular assertion, and t_{now} being the time of verification.

55. (NEW) A system for issuing certificates in a system for enforcing revocation in distributed systems, comprising:

- a) means for issuing certificates for principals within an organization by the organization;
- b) means for asserting, by the organization, a principal authorized as an authority for issuing time stamped certificates;
- c) means for delegating authority for issuing time stamped certificates;
- d) means for asserting freshness constraints on assertions; and
- e) means for verifying that a relation $|t_{now} - t_{time\ stamp}| \leq \delta$ is satisfied for each particular assertion necessary for verification of a secure channel, where $t_{time\ stamp}$ being a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification.

56. (NEW) A system for system security in a distributed system network, comprising:

- a) means for preparing a statement of an assigned revocation authority in a distributed system network in response to a policy, said revocation authority statement being associated with an initial statement;
- b) means for preparing a statement of a freshness constraint period in the distributed system network in response to said policy, said freshness statement being associated with said revocation authority statement;

c) means for preparing a validity statement at said assigned revocation authority in the distributed system network in response to said policy, said validity statement including a verification status at some temporal reference;

d) means for providing said revocation authority statement, said freshness statement, and said validity statement to a verification authority in the distributed system network; and

e) means for selectively verifying said initial statement at said verification authority in response to said initial statement, said revocation authority statement, said freshness statement, and said validity statement.

REMARKS

Consideration of the claims now in the case is requested. No new matter is added by this amendment.

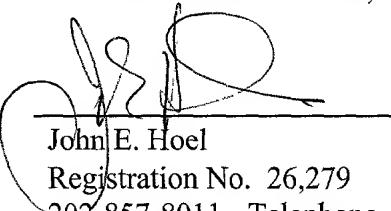
AUTHORIZATIONS

The Assistant Commissioner is hereby authorized to charge any additional fees which may be required for the timely consideration of this amendment under 37 C.F.R. §§ 1.16 and 1.17, or credit any overpayment to Deposit Account No. 13-4503, Order No. 2455-4230US3.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Dated: 4/23/01

By:


John E. Hoel
Registration No. 26,279
202-857-8011 - Telephone
202-857-7929 - Facsimile

SENDER'S ADDRESS:

Morgan & Finnegan L.L.P.
1775 Eye Street, N.W. Suite 400
Washington, D.C. 20006